What is Claimed is:

1. A method of generating computer security threat management information, comprising:

receiving notification of a computer security threat;

generating a computer-actionable Threat Management Vector (TMV) from the notification that was received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level; and

transmitting the TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

2. A method according to Claim 1 wherein the generating comprises selecting a system type, release level and possible countermeasures from a database that lists system types, release levels and possible countermeasures in a computer-readable format.

3. A method according to Claim 1 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

4. A method according to Claim 1 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

5. A method according to Claim 1 wherein at least one of the identifications comprises a pointer.

6. A method according to Claim 1 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level.

7. A method according to Claim 6 wherein the subsystem type comprises an application program type.

8. A method according to Claim 1 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat.

9. A system for generating computer security threat management information, comprising:

a Threat Management Vector (TMV) generator that is configured to generate a computer-actionable TMV from a notification of a computer security threat that is received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level.

10. A system according to Claim 9 wherein the TMV generator is also configured to transmit the TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

11. A system according to Claim 9 further comprising a common

semantics database that lists system types, release levels and possible countermeasures in a computer-readable format, wherein the TMV generator is responsive to the common semantics database to generate the TMV based upon user selection of a system type, release level and possible countermeasures from the common semantics database for the computer security threat.

12. A system according to Claim 9 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

13. A system according to Claim 9 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

14. A system according to Claim 13 wherein the set of possible countermeasures further comprises a pointer to a remediation to be applied as a countermeasure.

15. A system according to Claim 9 wherein the TMV further includes therein a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level.

16. A system according to Claim 15 wherein the subsystem type comprises an application program type.

17. A system according to Claim 9 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer

security threat.

18. A computer-actionable computer security Threat Management Vector (TMV) comprising:

a first computer-readable field that provides identification of at least one system type that is affected by a computer security threat;

a second computer-readable field that provides identification of a release level for the system type; and

a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level.

19. A TMV according to Claim 18 wherein the system type comprises a computer operating system type and wherein the release level comprises a computer operating system release level.

20. A TMV according to Claim 18 wherein the set of possible countermeasures comprises an identification of a countermeasure mode of installation.

21. A TMV according to Claim 18 wherein at least one of the identifications comprises a pointer.

22. A TMV according to Claim 18 further comprising:

a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat;

a fifth computer-readable field that provides identification of a release level for the subsystem types; and

wherein the third computer-readable field provides identification of a set of possible countermeasures for a subsystem type and a release level.

23. A TMV according to Claim 18 wherein the TMV further includes therein a sixth computer-readable field that provides identification of the computer security threat.